International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.127-136
http://dx.doi.org/10.14257/ijsia.2013.7.6.13

# A Novel Card-based Information Security Game Development on SNS

Woo-Taek Lim[1], Moon-Bo Yang[1] and Seong Baeg Kim[1,1]
[1] *Dept. of Computer Education, Jeju National University, Jeju-do, Republic of Korea*
*{longdari51,didansqh}@gmail.com, sbkim@jejunu.ac.kr*

***Abstract.***

*As smart appliances have developed rapidly, much convenience and information have been brought to people. However, as smart appliances become popular, conversely the problems of information security increase actually and the cognition of the information security decreases gradually. With the advance of smart appliances, one of the most developing systems is SNS (Social Network System). SNS exchanges much information through interaction and sharing with a lot of people. In this system, to improve the cognition of information security, it is required to develop a SNG (Social Network Game) adding edutainment on information security. This study aims to develop a novel card-based security information game connected with SNS, promote the awareness of the importance of private information management, and ultimately reduce the problems of information security by improving the cognition of the information security.*

***Keywords:*** *Information Security, SNS, SNG, Information Security Game, Smart Appliances, Edutainment*

## 1. Introduction

Recently, smart appliances such as smart phone and smart pad become popular increasingly. Compared with the existing IT appliances, smart appliances provide many advantages like touch user interface, mobile internet environment, and superior program development environment.

Since a computer becomes commercial, the negative sides of a computer including misuse of internet and internet game addition are increasing. An accident about information security has occurred frequently, but personal users even do not know how to deal with information security or crime like hacking.

Therefore, the education for information security is urgently required to realize the current level of information security. There is no doubt that information-oriented society brings much convenience. However, the problems including information exposure, invasion of privacy, fraud in e-commerce, and interruption of system operation have been more serious issue. Personal users who do not have professional knowledge of a computer are exposed to high possibility of being attacked in terms of information security. However, they actually do not realize well the risks of the attacks and how to protect themselves from it.

Current education about information security is mostly limited to computer experts who deal with information security, and its contents include only explanation of formal IT terms. As a result, the education for information security suited for nonprofessional

[1] Seong Baeg Kim (sbkim@jejunu.ac.kr) is the corresponding author of this paper.

ISSN: 1738-9976 IJSIA

users is insufficient in practice. Ironically, as this situation becomes more serious, nonprofessional users avoid the education rather than overcome the risks. Therefore, the first action to prevent security problems is that proper contents are needed to be provided not only for experts but also nonprofessional users. Contents should be offered to nonprofessional users for making them learn about hacking and preventing themselves from it.

Rapid development of smart appliances provides convenience and large amount of information. However, as smart appliances develop and take greater role in society, problems of information security also increase. As the operating systems of smart appliances have stronger security functions compared to the existing operating systems, the awareness of information security is lower relatively. One of the most common problems that occurred frequently in information security is an exposure of personal information. Thus, this problem of information security should be solved, and solutions to increase the awareness of importance of information security in order to prevent serious damages are required.

Social Network System (SNS) is largely developing along with the growth of smart appliances. SNS is largely exposed to the risk of information leaks as it shares information and communicates with others. Thus, a novel social network game which enhances awareness of information security on SNS is required to take attention. The reason why this study develops a social network game is that it can be utilized in advertising and marketing by connecting with social network system. In addition, the importance of managing personal information could be realized. Furthermore, the awareness of information security could be enhanced, so this may contribute to reducing security problems.

This study endeavored to create new ideas by considering the characteristics of learning contents. For example, the purpose of producing learning contents about hacking is for nonprofessional users to make them understand principles of hacking system easier and to increase awareness of information security.

Existing games related to information security have been produced by reflecting only one part of information security. Thus, contents are boring and results in poor educational effects. In this study, the way to produce information security game, which generates interests in managing personal information and increase the understanding of personal information leaks occurred by hacking, will be discussed. In addition, an information security game can connect with social network system, so a ranking system also can be used in the information security game. Therefore, it could arouse interests and competition. Furthermore, the game could be advertised easily by using the advantages of social network.

## 2. Background

One of the research works about a secure access to educational resources [1] focused on proposing an educational web model. Most of the security-related research consisted of the detailed description and theoretical knowledge [2, 3]. However, these researches didn’t consider an approach like a social network game for boosting the awareness of information security.

One of the most well-known hacking games is Uplink [8]. After examining the game, we found out that as the game progresses, it makes a gamer feel like doing an actual hacking. Since a lot of computer and network terminologies appear at the game and the game was created on the basis of the hacking principle, it is manly used by computer

professionals. Also, since an execution screen of Uplink does not include much information and even tutorial does not provide sufficient description, it is difficult to understand the game. Therefore, it is required to develop the game that is easy to understand and access for information security. Existing hacking games focus only on the game elements without considering any educational aspects. So the objective of the game is not clear due to focusing on only the game without a comprehensive approach of considering various aspects. IT system-oriented security from the 1990s has grown up in Korea, and then later was expanded into network security and personal information protection areas in 2004 and 2007, respectively [6].

Most of the information security games focus on the game attributes. As the result, the educational effects are little or unsustainable. Information security games, which were developed until now, are limited to the experts who work in the field of computer science, and it is so difficult for the non-experts to play them. So, in this study, we aim at developing a game, which can be understood and naturally approached by non-experts. We intend to imprint that they can manage and keep their personal information for themselves after playing the game [5]. In addition, we propose a ranking system that a lot of people can arouse a competitive spirit. Finally, by using social network systems, natural publicity and marketing for the game can be made easily. Therefore, our goal is to develop an information security game that includes the learning contents of hacking principles, linked with SNS.

The more specific descriptions for the game are at the following. First, Flash technology (Adobe AIR) is used for the development of the game. The game is started after setting up a computer as a defender and a gamer as an attacker. The gamer goes to the next stage through the processes of solving quizzes related to hacking principles. For example, when a gamer starts the game, the gamer can enter the gamer's personal information. Then, as the game continues, in case the gamer couldn't make a defense, the gamer's personal information would be a little bit exposed to the attacker. Second, using the connection with Facebook, which provides SNS services, easy publicity and marketing could be achieved and it could be popular through a ranking system that draws an active participation.

## 3. Design and Implementation

### 3.1. Overview

Edutainment improves learning immersion and achievement degree because it enables to learn a learner with interest and fun. Additionally, edutainment reduces the negative awareness of the game, which brings a game addiction or interferes with learning [4]. Due to the effects of edutainment, attention and research on it has been made continuously. However, there has been little edutainment for information security. Furthermore, there has been less edutainment contents or an edutainment plan suitable for smart appliances.

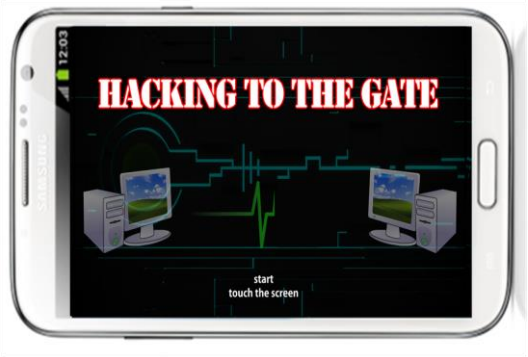
One of the most frequently occurring problems in the information security is related to the leakage of personal information. So, security-related games developed in this study are to be proceeded in a manner that after the computer sets as an attacker and a gamer sets as a defender, then, the gamer solves a simple quiz related to information security. If he/she cannot make a defense of his/her own personal information entered when he/she starts the game, the game goes on in the form that the personal information is exposed one by one to the attacker. As it goes on, the attack level of the attacker goes up gradually as well as the game points. The questions related to the hacking attacks

rather than actual hacking attacks are presented to the defender by the attacker. So the defender is able to move one step closer to information security and enjoy this game without difficulty.

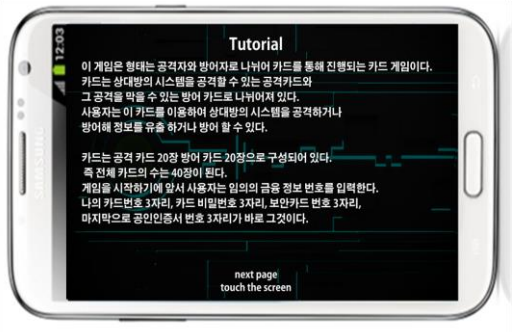
When you are ready to start the game, the screen that can enter your personal information will be displayed. The game will be started after a gamer enters his personal information. When the game is started, gamers are divided into an attacker and a defender. For example, the attacker would give a problem that causes an error difference by one and then the defender try to solve the problem. Let's think about the following question. If you want to create a fence of 100 meters, erect a pillar every 10 meters, how many pillars will be necessary? The correct answer is 11, but many people answer that the answer would be 10. This kind of error difference by one is called 'fencepost error' and this error occurs when the programmer misunderstood the number of items and the number of spaces between items [7]. As another example, there was a terminal communication program with safety in order to replace telnet, rsh, and rcp that are non-encrypted services. In this case, there was error difference by one in assigning the channels and thus the program was mainly targeted to make an attack.

So, in our information security game, the defender solves the quiz related to the hacking story. If the defender solves the quiz successfully, then the level goes up and the gamer gets more game points. Otherwise, the defender should expose the personal information one by one to the attacker. If the personal information of the defender is fully exposed, then the defender finally loses the game. After the game is finished, the defender can ascertain whether the personal information is well protected or not. Facebook is providing services to developers so that anyone can register more than one content. Then, by introducing a ranking system through the score using the service, and creating a security ranking list, it is possible to make the game more competitive so as to induce people.

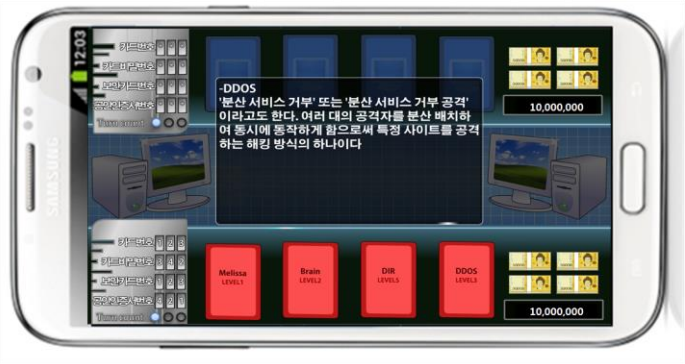
Figure 1 shows the screenshots of this game. This game is a kind of battle using cards. There are 40 cards in total that consist of half- attack and half-defense cards. The total number of cards can be flexible in case there is a new attack or defense in the future.




(a) Start screen




(b) Tutorial




(c) Main screen

**Figure 1. Screenshots of the Game Startup**

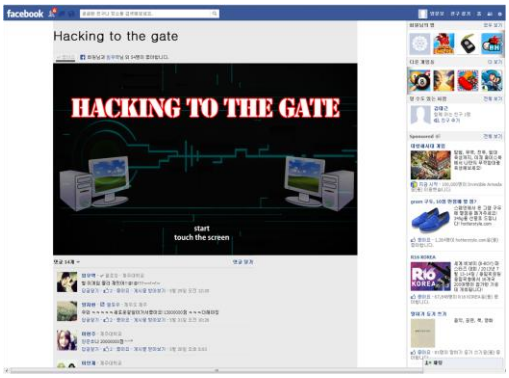



**Figure 2. Connection with Facebook on the Web**

**Figure 3. Ranking System**

We want to be able to manage a gamer's personal information so that it is possible to work with the Facebook game that contacts with anyone, exit via Facebook with the game. Figure 2 represents the screenshot, which shows that the hacking game is registered on Facebook. It tells that everyone can participate in the game and the natural promotion effect is straightforward, and all participants can write a response message. Figure 3 shows that gamers can announce security ranking and share each other through ranking page.

### 3.2. Game Scenario

This study developed a card game about information security. Cards contain negative contents related to information security and solutions. Now the scenario of the card game is as follows.

In this game, a user and a computer play in a confrontation. The user and computer may set their unique numbers when they start a game. The unique numbers consist of card number, security card number, and authentication certificate number. Each number has three digits. Their own unique numbers are personal information. When numbers are set, a certain amount of basic money is given and the game starts.

Figure 4 shows the screen where a user sets numbers before a game starts. Figure 5 shows the screen where a user and a computer play in a confrontation when a game

starts. A user and a computer are given each four cards randomly. The user and computer play a turn including attack and defense. The user picks a card out of four and attacks the computer or defends himself/herself against the computer. After an attack or a defense, the user has to discard a card and receives a random card. This game is organized in this way to make the user realize factors of the game.

As the game progresses, the turn is changed when three defenses are successful like three outs in baseball. Since this card game progresses in a confrontation, game cards are divided into attacker cards and defender cards. The attacker cards contain hacking, virus, and malignant code and the defender cards contain solutions for each attacker card. Also, each card has a level. The higher level a card has, the higher attack and defense it has. The higher level a card has, the more powerful hacking it describes.

If the user or computer in a confrontation attacks the other successfully, the user or computer can find the opposite's unique number. Once the user or computer finds the number, he/she can take the other's capital. The other's capital is added to one's capital. Then, the whole capital is the key to decide who the winner is. Also, the one who takes all of the other's capital wins the game immediately. Figure 6 is the screen that shows random quiz questions related to information security during the game in order to emphasize characteristics of edutainment. If a user gives a correct answer, a card with a higher level is given.

Through the game developed in this study, users learn how to attack the computer and types of attack and they learn how to defend themselves against each attack. They can also acknowledge serious leakage of personal information and develop how to cope with it.

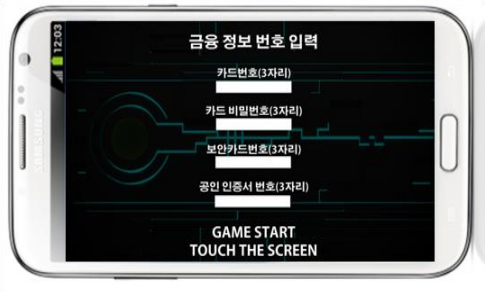



**Figure 4. Setting the Number of Screen**

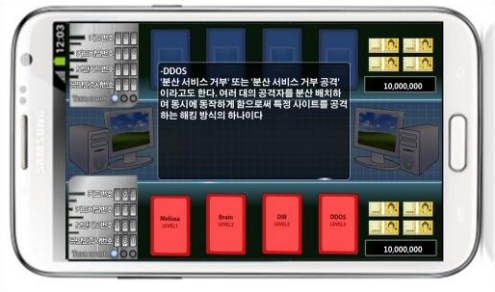



**Figure 5. Confrontation Screen**

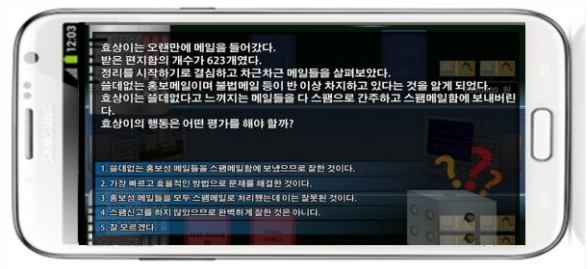



**Figure 6. Quiz Screen**

### 3.3. Game Interface Design

The interface of this card game was built in order for users to notice it at a glance and to understand it easily. Figure 7 shows that the user is not at the top but at the bottom so that it is easy for the user to play the game. On the bottom left for the user, the number set by the user is indicated and the number of outs is indicated as well. Also, on the bottom right, the capital owned by the user is indicated. A confrontation of cards takes place in the center of the screen.

While attacker cards are red to indicate attack, defender cards are blue to indicate defense. Also, in order to help users concentrate on the game, sparks fly off for an attack and a barrier spreads for a defense. When an attack is successful, a blue screen shows up in the game so that one realizes that he/she is attacked.

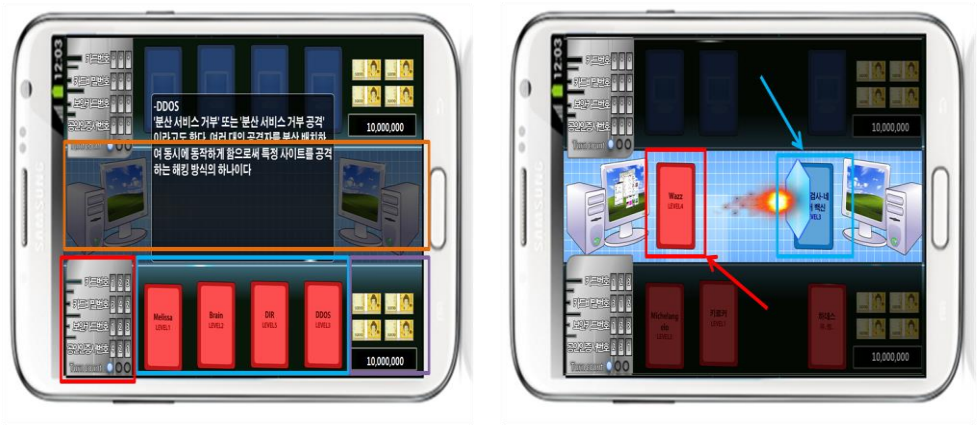



**Figure 7. Game Interface Screen**

### 3.4. Game Implementation

The game was implemented by using Adobe Flash and Action Script 3.0. The number of cards is 40 in total: 20 cards for attack and 20 cards for defense. Background images and card images were made simple by using Adobe Photoshop. When a user puts a cursor on a card image, the detailed description of the card shows up. In this way, the user can acquire a lot of knowledge about information security. Since the card game may be boring, many animation and graphic effects were added. The game was fabricated in order for users to play lively games.

Figure 8 shows how this game fabricated in Adobe Flash is connected to Facebook on the smart phone, so that more users have easy access to the game. Also, with 'likes' and 'comments', many opinions can be viewed; this will bring natural promotion effects. Figure 9 shows how the game developed in this study is uploaded to another user's Facebook when the user likes the game.

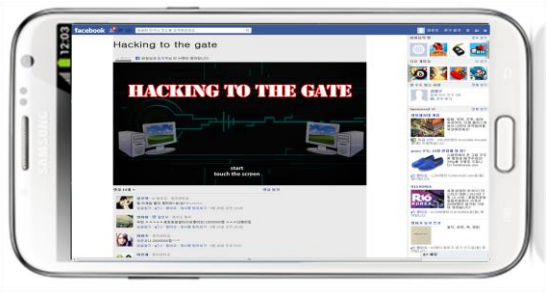



**Figure 8. Connection with Facebook on the Smart Phone**

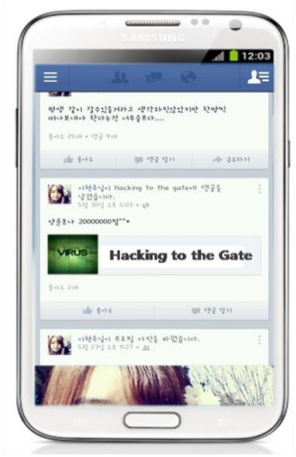



**Figure 9. Facebook Upload**

## 4. Conclusion

In this paper, we designed and developed a card-based game for information security, which enables people to understand information security knowledge and to boot the cognition of information security. The rapid development of smart devices offers a lot of convenience and information. We expect that the importance of information security industry will increase in the future. Through a security information game in conjunction with SNS, it's possible to recognize the importance of personal information management. We aimed to recognize the importance of personal information management to the non-expert. Then, by boosting awareness of information security, the issues of information security will be reduced. Finally, we expect that our research result will make a contribution to solve the information security issues and bring the advance of information culture.

For further study, we will continue to add new cards reflecting the emerging issues in the field of information security such as new hacking skills, information security problems, and solutions to cope with them. Also, we will analyze the effects of our card game after applying it to people.

## Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013009428)

## References

[1] O. N. Qunoo and H. Hamad, "Secure Model for Educational Resources", International Journal of Security and Its Applications, vol. 7, no. 1, **(2013)**, pp. 31-50.
[2] J. Piao and S. B. Kim, "The Design and Analysis of a Hardware-based Anomaly Detection Scheme", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 367-372.
[3] S. Song, H. Park and B. Choi, "E-LPG: Energy Efficient Location Privacy Scheme Against Global Attackers in Sensor Networks", Secure Model for Educational Resources. In: International Journal of Security and Its Applications, vol. 7, no. 2, **(2013)**, pp. 27-46.
[4] T. Lee, D. Kim, M. Lee and H. Peter, "Markov Chain Model-Based Trainee Behavior Pattern Analysis for Assessment of Information Security Exercise Courses", Journal of Information Science, vol. 16, no. 12. **(2010)**.

[5] T. Y. Youn and D. Hong, "Profile Management System for Contact Information Privacy in Social", Electronics and Telecommunications Research Institute, **(2011)**.
[6] D. Y. Maeng and J. K. Kwan, "Requirements for Activation of the Information Security Industry Knowledge of Korea", Journal of Korean Association for Regional Information Society, vol. 13, no. 1, **(2010)**.
[7] J. Erickson, "Hacking: the Art of Exploitation", Acorn Publishing Co. **(2011)**.
[8] Uplink home page, http://www.introversion.co.uk/uplink.

## Authors

**Woo-Taek Lim**, he is currently an undergraduate student of the Dept. of Computer Education at Jeju National University. He is the student president of the Dept. of Computer Education student council. His research interests include computer science education and computer security education.

**Moon-Bo Yang**, he is currently an undergraduate student of the Dept. of Computer Education at Jeju National University. He is the student vice-president of the Dept. of Computer Education student council. His research interests include computer science education and computer security education.

**Seong Baeg Kim**, Professor Kim received the B.S., M.S., and Ph.D. in Computer Engineering from Seoul National University, Korea, in 1989, 1991, and 1995 respectively. He is currently a professor of the Dept. of Computer Education at Jeju National University, where he has been since 1996. He was a visiting scholar at Dept. of Computer Science, Montana State University from 2001 to 2002 and Dept. of Electrical & Computer Engineering, University of Cincinnati from 2008 to 2009. His research interests include computer science education, computer system architecture, and computer security.